PTO 06-5499

World Patent
Document No. WO 99/41657

# METHOD FOR PREVENTING ILLEGAL COPYING OF COMPUTER SOFTWARE

[Konpyuta Sofutowea no Iho Kopi Boshi Hoho]

Kunio Shiba

UNITED STATES PATENT AND TRADEMARK OFFICE
Washington, D.C. July 2006

Translated by: Schreiber Translations, Inc.

| | | |
|---|---|---|
| Country | : | Japan |
| Document No. | : | WO 99/41657 |
| Document Type | : | Kokai |
| Language | : | Japanese |
| Inventor | : | Kunio Shiba |
| Applicant | : | Kunio Shiba |
| IPC | : | G 06 F 9/06 |
| Application Date | : | October 12, 1998 |
| Publication Date | : | August 19, 1999 |
| Foreign Language Title | : | Konpyuta Sofutowea no Iho Kopi Boshi Hoho |
| English Title | : | METHOD FOR PREVENTING ILLEGAL COPYING OF COMPUTER SOFTWARE |

/1[1]

(54) Title of the invention /0

METHOD FOR PREVENTIGN ILLEGAL COPYING OF COMPUTER SOFTWARE

(57) Abstract

A first recording medium (3) on which computer software has been recorded and an encodable second recording medium (4) are used, on an installing occasion, for recording, onto the aforementioned second recording medium, a unique volume serial No. VSN (HD) assigned preliminarily to the recording medium (2) of a given hardware member as the decodable installation information No. IIN (HD) of said hardware member, whereas the volume serial No. of the recording medium of the hardware member and the hardware installation information No. recorded onto the second recording medium are compared on a re-installing occasion, and it becomes possible, by preventing installation & identifying the hardware member in a case where the respective numbers differ, to prevent illegal copying onto many hardware members.

Specification /1

Method for preventing illegal copying of computer software

Technical fields

The present invention concerns a method for preventing so-called "illegal copying," namely the copying a singular computer software program onto multiple hardware members.

Technical background

Generally speaking, commercial computer software is sold in a morphology whereby it is permitted to be copied (installed) onto a singular hardware member (computer) alone.

---

[1] Numbers in the margin indicate pagination in the foreign text.

In reality, however, computer software can be installed onto multiple hardware members by using a singular recording medium onto which said software has been recorded.

As a measure for preventing installation onto multiple hardware members, furthermore, a method wherein a serial No. is assigned to every product and wherein the input of said serial No. is mandated at the time of installation is being practiced, although since this serial No. represents information known to a user purchasing each product, this measure is incapable of preventing installations onto other hardware members, and in a case where a user purchasing a product has informed, together with said product, other users of the serial No. thereof, furthermore, it is impossible to prevent illegal copying.

Measures for preventing illegal copying by notifying uses of the illegality of such an act via user permits, etc. are also practiced, although since this measure relies on users' discretion, practical efficacies cannot be realistically expected.

A recording medium onto which computer software has been recorded, furthermore, can be easily duplicated, based on which installations onto larger numbers of hardware members become possible.

One objective of the present invention is therefore to provide a method for preventing illegal copying of computer software capable of forcibly preventing installations of computer software onto multiple hardware members. /2

Another objective, furthermore, is to provide a method for preventing illegal copying of computer software capable, in a case where an attempt is made to install computer software by using a duplicated recording medium, of forcibly preventing this installation.

Disclosure of the invention

The present invention is constituted, by using a first recording medium on which computer software has been recorded and an encodable second recording medium, to record, onto the aforementioned second recording medium, the unique volume serial No. assigned preliminarily to

the recording medium of a given hardware member as the decodable installation information No. of said hardware member on an installing occasion, to compare, on a re-installing occasion, the volume serial No. of the recording medium of the hardware and the hardware installation information No. recorded onto the second recording medium, and, in a case where the respective numbers differ, to prevent installation.

The volume serial No. hereby assigned to the recording medium of the hardware member is randomly & automatically assigned to said recording medium by formatting software at the time of formatting the former and may, for example, be constituted a 9-digit number.

The probability of assignments of identical volume serial Nos. is therefore extremely low, and in a case where this volume serial No. is recorded, onto the second recording medium, as the installation information No. of the recording medium of the hardware member on an initial installing occasion and where the installation information No. of the hardware member targeted on a re-installing occasion is compared with the installation information No. of the already installed hardware member, it becomes possible to judge whether or not the hardware member targeted for re-installation is the legally installed hardware member and therefore to prevent illegal copying onto multiple different hardware members.

The present invention may, furthermore, be constituted to record, onto the second recording medium, the unique volume serial No. assigned preliminarily to the aforementioned first recording medium as the decodable installation information No. of said first recording medium, to compare, on an installing occasion, the unique volume serial No. assigned preliminarily to the aforementioned first recording medium with the installation information No. of said first recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, to prevent installation. /3

As far as this embodiment is concerned, in a case where the first recording medium is duplicated and where an installation attempt is then made by using the first recording medium thus duplicated together with an unused second recording medium, a volume serial No. different from

the authentic installation information No. corresponding to the first recording medium has been assigned to the duplicated first recording medium, and therefore, in a case where said volume serial No. differs from the installation information No. of the first recording medium recorded onto the second recording medium, the first recording medium becomes judged to be a duplicate, based on which illegal copying can be prevented.

The present invention may, furthermore, be constituted to record, onto the aforementioned second recording medium, the unique volume serial No. assigned preliminarily to said second recording medium as the decodable installation information No. of said second recording medium, to compare, on an installing occasion, the unique volume serial No. assigned preliminarily to the aforementioned second recording medium with the installation information No. of said second recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, to prevent installation.

As far as this embodiment is concerned, in a case where the second recording medium is duplicated and where an installation attempt is then made by using the second recording medium thus duplicated, the authentic installation information No. becomes copied onto the duplicated second recording medium, but since a volume serial No. different from the authentic installation information No. which corresponds to said second recording medium and which has been recorded onto said second recording medium has been assigned to said second recording medium, the second recording medium becomes judged to be a duplicate in a case where said volume serial No. differs from the installation information No. of the second recording medium recorded onto said second recording medium, based on which illegal copying can be prevented.

The present invention may, furthermore, be constituted, by using an encodable recording medium onto which computer software has been recorded, to record, onto the aforementioned recording medium, the unique volume serial No. assigned preliminarily to the recording medium of a hardware member as the decodable installation information No. of said hardware member on an installing occasion, to compare, on a re-installing occasion, the volume serial No. of the recording

medium of said hardware member with the installation information No. of said hardware member recorded onto said recording medium, and, in a case where the respective numbers differ, to prevent installation.

As far as this embodiment is concerned, the volume serial No. of the hardware member is /4 recorded onto the second recording medium as the installation information No. thereof on the initial installing occasion, and the installation information No. of a hardware member targeted for installation on a re-installing occasion is compared with the installation information No. of the already installed hardware member which has been recorded onto the second recording medium, based on which it becomes possible to judge whether or not the hardware member targeted for re-installation is the legally installed hardware member and therefore to prevent illegal copying onto multiple different hardware members.

The present invention may, furthermore, be constituted to record, onto the aforementioned recording medium, the unique volume serial No. assigned preliminarily to said recording medium as a decodable installation information No., to compare, on an installing occasion, the aforementioned volume serial No. with the recorded installation information No.., and, in a case where the respective numbers differ, to prevent installation.

As far as this embodiment is concerned, in a case where a recording medium onto which computer software has been recorded is duplicated and where an installation attempt is then made by using the recording medium thus duplicated, the authentic installation information No. becomes copied onto the duplicated recording medium, but since a volume serial No. different from the authentic installation information No. which corresponds to the second recording medium and which has been recorded onto said [authentic] recording medium becomes assigned to said duplicated recording medium, it becomes possible, in a case where this volume serial No. differs from the installation information No. of the second recording medium recorded onto said second recording medium, to judge that said second recording medium is a duplicate and therefore to prevent illegal copying.

The present invention may, furthermore, be constituted, by encrypting the aforementioned installation information No. and by thus preventing the tampering of the installation information No., to secure further improved illegal copying prevention effects.

Brief explanation of the figures

Figure 1 is an approximate diagram which shows the constitution of a system orchestrated for implementing the present invention.

Figure 2 is an approximate diagram which shows the volume serial No. & installation information No. recording states of a recording medium used for the first application embodiment of the present invention.

Figure 3 is a routine flow diagram pertaining to the first application embodiment of the present invention.

Figure 4, which is provided for explaining the second application embodiment of the present invention, is an approximate diagram which shows the volume serial No. & installation information No. recording states of a recording medium used for the same. /5

Figure 5 is a routine flow diagram pertaining to the second application embodiment of the present invention.

Figure 6, which is provided for explaining the third application embodiment of the present invention, is an approximate diagram which shows the volume serial No. & installation information No. recording states of a recording medium used for the same.

Figure 7 is a routine flow diagram pertaining to the third application embodiment of the present invention.

Figure 8 is a routine flow diagram pertaining to the fourth application embodiment of the present invention.

Figure 9 is another routine flow diagram pertaining to the fourth application embodiment of the present invention.

Optimal embodiments for implementing the invention

The present invention will be explained with reference to attached figures for the purpose of providing more detailed explanations.

Figure 1 through Figure 3 show the first application embodiment of the present invention, according to which major components of the present application embodiment are constituted by the computer (1) outfitted with the hard disc (HD) (2), which is targeted for computer software installation, the CD-ROM (CD) (3), which serves as a read-only first recording medium onto which said computer software has been recorded, and the floppy disc (FD) (4), which serves as an encodable second recording medium.

Additionally configured on the aforementioned computer (1) are the CD-ROM drive (5) designed to decode the aforementioned CD (3) and the floppy disc drive (6) designed to decode the aforementioned FD (4).

As far as the present application embodiment is concerned, furthermore, a volume serial No. VSN (CD1) & a volume serial No. VSN (FD1) assigned randomly & automatically on their respective formatting occasions, have, as Figure 1 (b) indicates, been recorded onto the aforementioned CD (3) & FD (4), whereas the aforementioned volume serial No. VSN (CD1) & volume serial No. VSN (FD1) have, furthermore, been recorded onto the FD (4) as sets of decodable information, namely installation information Nos. IIN (CD1) & IIN (FD1).

Recorded onto the aforementioned HD (5), furthermore, is the volume serial No. VSN (HD1) assigned randomly & automatically at the time of the formatting thereof.

This volume serial No. VSN is normally constituted by a 9-digit decimal number, and the /6 probability of assignments of individual volume serial Nos. is 1/999,999,999.

Moreover, the aforementioned probability can be further elevated [sic: Presumably "lowered"] by encrypting this number by means of an arbitrary computation.

Next, the first application embodiment of the present invention designed to use these major constituent components will be explained with reference to the routine flow chart of Figure 3.

First, the CD (3) & FD (4) are inserted into the computer (1) targeted for computer software installation, and the installation may, for example, be initialized by loading an installer recorded onto the CD (3).

Upon the commencement of this installation, the installation information No. IIN (HD1) of the HD (2) saved within the FD (4) is decoded (step S1), followed by the judgment of whether or not this IIN (HD1) has been recorded (step S2), and in a case where said IIN (HD1) has not been recorded, the pervasion of the first installing occasion is judged, and after the aforementioned IIN (HD1) has been recorded onto the FD (4) at the next step S3, the installation into the HD (2) is executed (step S4), as a result of which the routines become concluded.

In a case where the first installation attempt is thus made by using the authentic CD (3) & FD (4), the volume serial No. VSN (HD1) of the installation-completed HD (2) becomes, as Figure 2 indicates, recorded onto the FD (4) as the installation information No. IIN (HD1).

In a case where the IIN (HD1) is judged to have been recorded onto the FD (4) at the aforementioned step S2, on the other hand, it is judged that the first installation attempt has already been executed in relation to a given hardware member, and upon the completion of transition to the next step S5, the VSN (HD1) of the HD (2) of said computer (1) is decoded, followed by the comparison of the VSN (HD1) decoded from said HD (2) with the IIN (HD1) decoded from the FD (4) (step S6), and, granted that they are mutually identical, a transition to the step S4 is made, where the installation is permitted, whereas in a case where the respective Nos. are judged to be mutually different, the pervasion of a hard disc other than the installation-permitted one is judged, and after the installation has been rejected (step S7), the routines are completed.

In other words, in a case where these routines are executed, the computer (1) targeted for installation is indiscriminately subjected to installation on the initial installing occasion where the /7 authentic CD (3) & FD (4) are used, whereas upon the completion of the first installing occasion, only the initially installed computer (1) is permitted re-installation, based on which illegal copying can be prevented.

Next, the second application embodiment of the present invention will be explained with reference to Figure 4 & Figure 5.

The present application embodiment instantiates the copying prevention method of a case where an installation attempt is made by using a duplicated CD (3), whereas in a case where the CD (3) becomes duplicated, all sets of information recorded onto the authentic CD (3) become copied onto the duplicated CD (3), although a volume serial No. VSN (CD2) different from that of the authentic CD (3) has, as Figure 4 indicates, been assigned to this duplicated CD (3).

In a case where the installation becomes initialized by using the duplicated CD (3) together with the authentic FD (4), the authentic IIN (CD1) of the CD (3) recorded onto the FD (4) is initially decoded (step S10), followed by the decoding of the volume serial No. VSN (CD) of the CD (3) (step S11) and then by the comparison of said IIN (CD1) & VSN (CD) (step S12).

In a case where these Nos. are mutually identical, namely where the decoded VSN (CD) = volume serial No. VSN (CD1) of the authentic CD (3) = authentic installation information No. IIN (CD1) is ascertained, the inserted CD (3) becomes judged to be the authentic CD, followed by a transition to the next step S13, where the installation is permitted, and the routines are concluded.

VSN (CD2) has, on the other hand, been assigned as the volume serial No. of the duplicated CD (3), and since the decoded VSN (CD) = VSN (CD2) $\neq$ authentic CD (3) volume serial No. VSN (CD1) = authentic installation information No. IIN (CD1), namely decoded VSN (CD) = VSN (CD2) $\neq$ authentic IIN (CD1), becomes judged at the step S12, and since the inserted CD (3) thus becomes judged to be a duplicate (step S14), the installation is rejected, and the routines are concluded.

It becomes possible, according to these routines, to avoid installation by the duplicated CD (3).

Moreover, the third application embodiment of the present invention will be explained with reference to Figure 6 & Figure 7. /8

The present application embodiment instantiates the copying prevention method of a case where installation is executed by using a duplicated FD (4), whereas in a case where the FD (4) becomes duplicated, all sets of information recorded onto the authentic FD (4) become copied onto the duplicated FD (4), although a volume serial No. VSN (FD2) different from that of the authentic FD (4) has, as Figure 6 indicates, been assigned to this duplicated FD (4), although the authentic installation information Nos. IIN (CD1) & IIN (FD1) recorded onto the authentic FD (4) become copied onto this duplicated FD (4).

In a case where the installation is initialized by using the duplicated FD (4) together with the authentic CD1, the authentic IIN (FD1) of the FD (4) recorded onto the FD (4) becomes initially decoded (step S20), followed by the decoding of the volume serial No. VSN (FD) of the FD (4) (step S21) and then by the comparison of the IIN (FD1) & VSN (FD) (step S22).

In a case where the respective Nos. are mutually identical, namely where the decoded VSN (FD) = volume serial No. VSN (FD1) of the authentic FD (4) = authentic installation information No. IIN (FD1) is ascertained, the inserted FD (4) becomes judged to be the authentic FD, followed by a transition to the next step S23, where the installation is permitted, and the routines are concluded.

VSN (FD2) has, on the other hand, been assigned as the volume serial No. of the duplicated FD (4), and since the decoded VSN (FD) = VSN (FD2) $\neq$ volume serial No. VSN (FD1) of the authentic FD (4) = authentic installation information No. IIN (FD1), namely the decoded VSN (FD) = VSN (FD2) $\neq$ authentic IIN (FD1), becomes judged at the step S22, the inserted FD (4) becomes judged to be a duplicate (step S24), as a result of which the installation is rejected, and the routines are concluded.

It becomes possible, according to these routines, to avoid installation by the duplicated FD (4).

Thus, the present invention is capable not only of preventing installations into multiple different computers (1) but also of preventing installations based on the use of the duplicated CD /9

(3) or FD (4).

Incidentally, a case where the respective routines for preventing installations into multiple different computers (1) and for preventing installations by using the duplicated CD (3) or FD (4) are executed separately has been instantiated by each of the aforementioned application embodiments, although it is also possible to execute these routines consecutively according to the illustrations of Figure 8 & Figure 9.

According to these figures, steps S30 through S33 represent routines executed in relation to a duplicated FD, whereas steps S34 through S37 represent routines executed in relation to a duplicated CD, whereas steps S38 through S44 represent routines for preventing installations in relation to multiple different computers (1).

These series of routines can prevent all conceivable illegal copying acts.

It goes without saying, furthermore, that these illegal copying prevention methods are equally applicable to a case where computer software has been recorded onto a singular encodable recording medium (e.g., singular FD or singular CDR).

In the case of a CD-ROM used, upon the shipping thereof, as a read-only & encoding-disabled recording medium, furthermore, it becomes possible, by decoding, at the time of the manufacture of said CD-ROM, namely of encoding computer software, the unique volume serial No. assigned to said CD-ROM and by encoding, together with said computer software, this volume serial No. as an installation information No., to compare, on an installing occasion, the aforementioned volume serial No. & installation information No. and, in a case where the respective numbers differ, to prevent the illegal copying of the singular CD-ROM by rejecting installation.

Industrial application possibilities

As has been mentioned above, the present invention is capable, in a case where computer software is sold in a state where it has become recorded onto a recording medium, to prevent illegal copying both forcibly & assuredly based on integration with the installer thereof.

Patent Claims /10

1. A method for preventing illegal copying of computer software characterized by the recording, by using a first recording medium on which computer software has been recorded and an encodable second recording medium & onto the aforementioned second recording medium, a unique volume serial No. assigned preliminarily to the recording medium of a hardware member as the decodable installation information No. of said hardware member on an installing occasion, by the comparison, on a re-installing occasion, of the volume serial No. of the recording medium of the hardware member and the hardware installation information No. recorded onto the second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

2. A method for preventing illegal copying of computer software specified in Claim 1 characterized by the recording, onto the second recording medium, of the unique volume serial No. assigned preliminarily to the aforementioned first recording medium as the decodable installation information No. of said first recording medium, by the comparison, on an installing occasion, of the unique volume serial No. assigned preliminarily to the aforementioned first recording medium with the installation information No. of said first recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

3. A method for preventing illegal copying of computer software specified in Claim 1 or 2 characterized by the recording, onto the aforementioned second recording medium, of the unique volume serial No. assigned preliminarily to said second recording medium as the decodable installation information No. of said second recording medium, by the comparison, on an installing occasion, of the unique volume serial No. assigned preliminarily to the aforementioned second recording medium with the installation information No. of said second recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

4. A method for preventing illegal copying of computer software characterized by the recording, by using an encodable recording medium onto which computer software has been

recorded & onto the aforementioned recording medium, of the unique volume serial No. assigned preliminarily to the recording medium of a hardware member as the decodable volume serial No. of said hardware member on an installing occasion, by the comparison, on a re-installing occasion, of the volume serial No. of the recording medium of said hardware member with the installation information No. of said hardware member recorded onto said recording medium, and, in a case where the respective numbers differ, by the prevention of installation. /11

5. A method for preventing illegal copying of computer software specified in Claim 4 characterized by the recording, onto the aforementioned recording medium, of the unique volume serial No. assigned preliminarily to said recording medium as a decodable installation information No., by the comparison, on an installing occasion, of the aforementioned volume serial No. with the recorded installation information No., and, in a case where the respective numbers differ, by the prevention of installation.

6. A method for preventing illegal copying of computer software specified in any of Claims 1 through 5 characterized by the encryption of the aforementioned installation information No.

7. A method for preventing illegal copying of computer software characterized, at the time of the manufacture of a read-only recording medium onto which computer software has been recorded, by the recording, into the aforementioned computer software, the unique volume serial No. assigned preliminarily to the aforementioned recording medium as an installation information No., by the comparison, on an installing occasion, of the aforementioned volume serial No. with the installation information No. recorded into the computer software, and, in a case where the respective numbers differ, by the prevention of installation.

Patent Claims of Amendment Form /12

[Received by the International Office on April 8, 1999; new Claims 8, 9, & 10 are added; no changes in the other Claims (2 pages)]

Patent Claims

1. A method for preventing illegal copying of computer software characterized by the recording, by using a first recording medium on which computer software has been recorded and an encodable second recording medium & onto the aforementioned second recording medium, a unique volume serial No. assigned preliminarily to the recording medium of a hardware member as the decodable installation information No. of said hardware member on an installing occasion, by the comparison, on a re-installing occasion, of the volume serial No. of the recording medium of the hardware member and the hardware installation information No. recorded onto the second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

2. A method for preventing illegal copying of computer software specified in Claim 1 characterized by the recording, onto the second recording medium, of the unique volume serial No. assigned preliminarily to the aforementioned first recording medium as the decodable installation information No. of said first recording medium, by the comparison, on an installing occasion, of the unique volume serial No. assigned preliminarily to the aforementioned first recording medium with the installation information No. of said first recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

3. A method for preventing illegal copying of computer software specified in Claim 1 or 2 characterized by the recording, onto the aforementioned second recording medium, of the unique volume serial No. assigned preliminarily to said second recording medium as the decodable installation information No. of said second recording medium, by the comparison, on an installing occasion, of the unique volume serial No. assigned preliminarily to the aforementioned second recording medium with the installation information No. of said second recording medium recorded onto said second recording medium, and, in a case where the respective numbers differ, by the prevention of installation.

4. A method for preventing illegal copying of computer software characterized by the recording, by using an encodable recording medium onto which computer software has been

recorded & onto the aforementioned recording medium, of the unique volume serial No. assigned preliminarily to the recording medium of a hardware member as the decodable volume serial No. of said hardware member on an installing occasion, by the comparison, on a re-installing occasion, of the volume serial No. of the recording medium of said hardware member with the installation information No. of said hardware member recorded onto said recording medium, and, in a case where the respective numbers differ, by the prevention of installation. /13

5. A method for preventing illegal copying of computer software specified in Claim 4 characterized by the recording, onto the aforementioned recording medium, of the unique volume serial No. assigned preliminarily to said recording medium as a decodable installation information No., by the comparison, on an installing occasion, of the aforementioned volume serial No. with the recorded installation information No., and, in a case where the respective numbers differ, by the prevention of installation.

6. A method for preventing illegal copying of computer software specified in any of Claims 1 through 5 characterized by the encryption of the aforementioned installation information No.

7. A method for preventing illegal copying of computer software characterized, at the time of the manufacture of a read-only recording medium onto which computer software has been recorded, by the recording, into the aforementioned computer software, the unique volume serial No. assigned preliminarily to the aforementioned recording medium as an installation information No., by the comparison, on an installing occasion, of the aforementioned volume serial No. with the installation information No. recorded into the computer software, and, in a case where the respective numbers differ, by the prevention of installation.

8. [Added] A method for preventing illegal copying of computer software specified in any of Claims 1 through 7 characterized by the encryption of the aforementioned volume serial No.

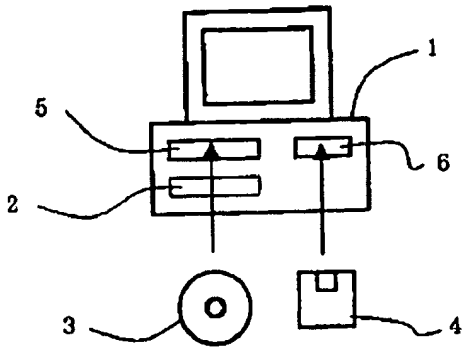
9. [Added] A method for preventing illegal copying of computer software characterized, with regard to the method for preventing illegal copying of computer software specified in any of

Claims 1 through 8, by the designation, as the installation information No., of the identification No. assigned to the hardware in place of the aforementioned volume serial No.

10. [Added] A method for preventing illegal copying of computer software characterized, with regard to the method for preventing illegal copying of computer software specified in any of Claims 1 through 8, by the designation, as the installation information No., of an identification No. assigned to the CPU of the hardware in place of the aforementioned volume serial No.

Figures 1 /14

(a)




(b)

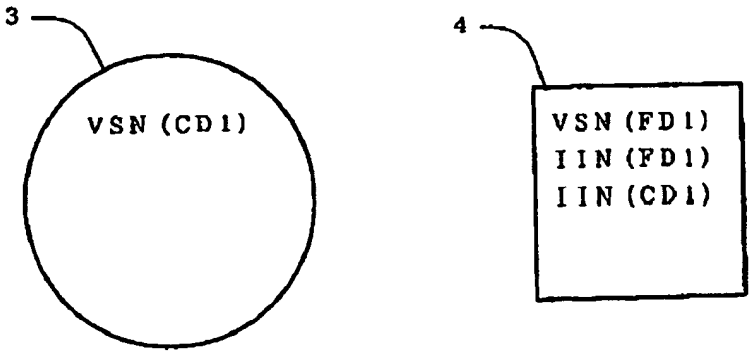



Figure 2 /15

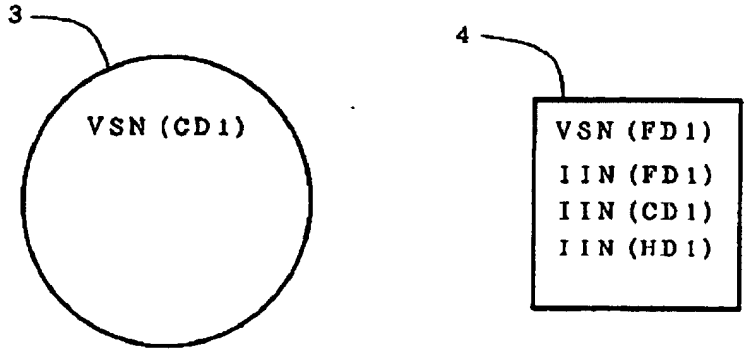
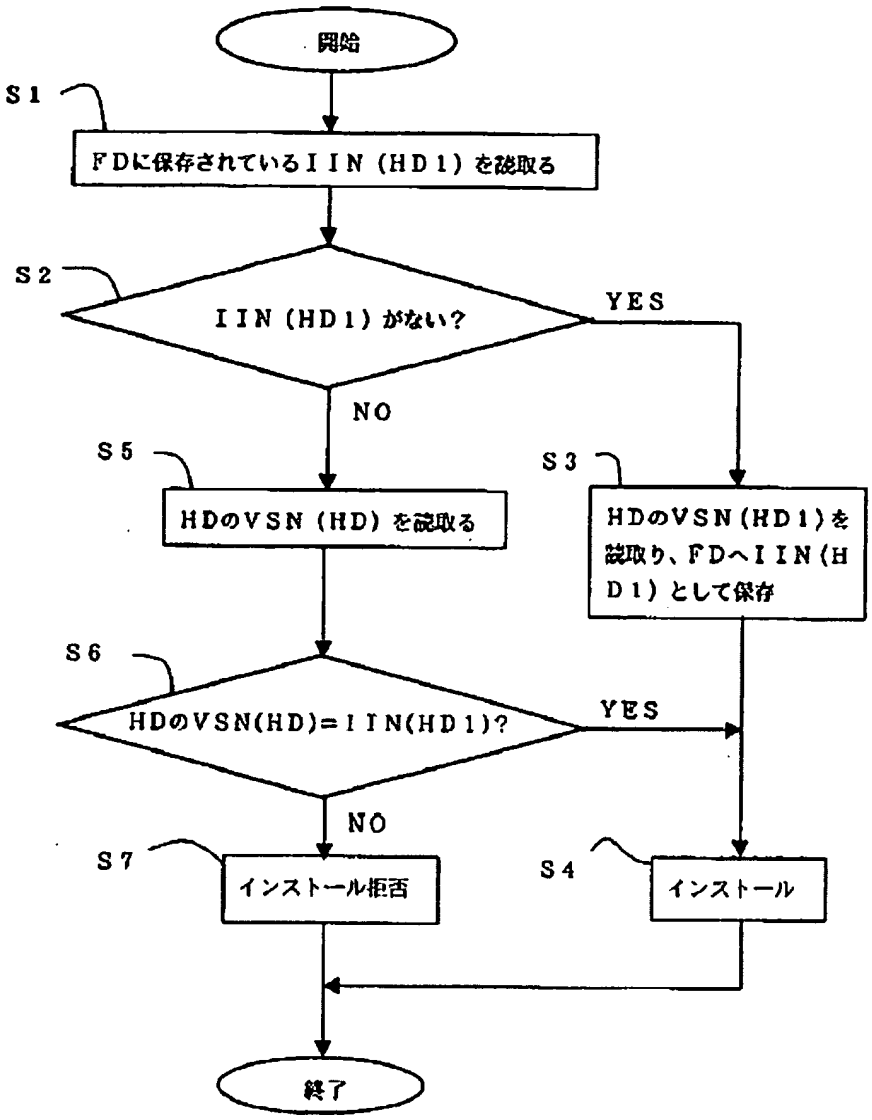



Figure 3 /16




[(A): Begin; (B): End; (S1): Decode IIN (HD1) saved in FD; (S2): IIN (HD1) absent?; (S3): Decode VSN (HD1) of HD and save same into FD as IIN (HD1); (S4): Install; (S5): Decode VSN (HD) of HD; (S6): VSN (HD) of HD = IIN (HD1)?; (S7): Reject installation]

Figure 4 /17

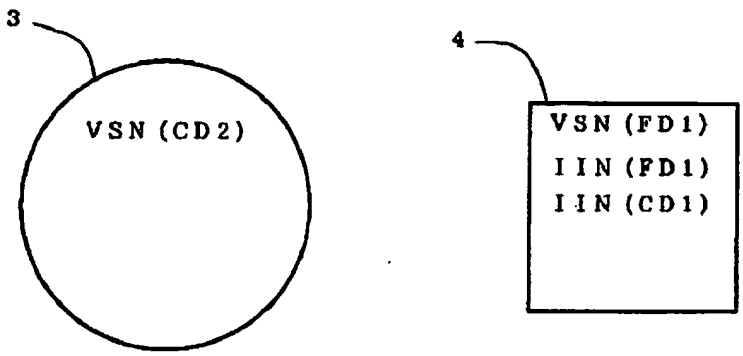
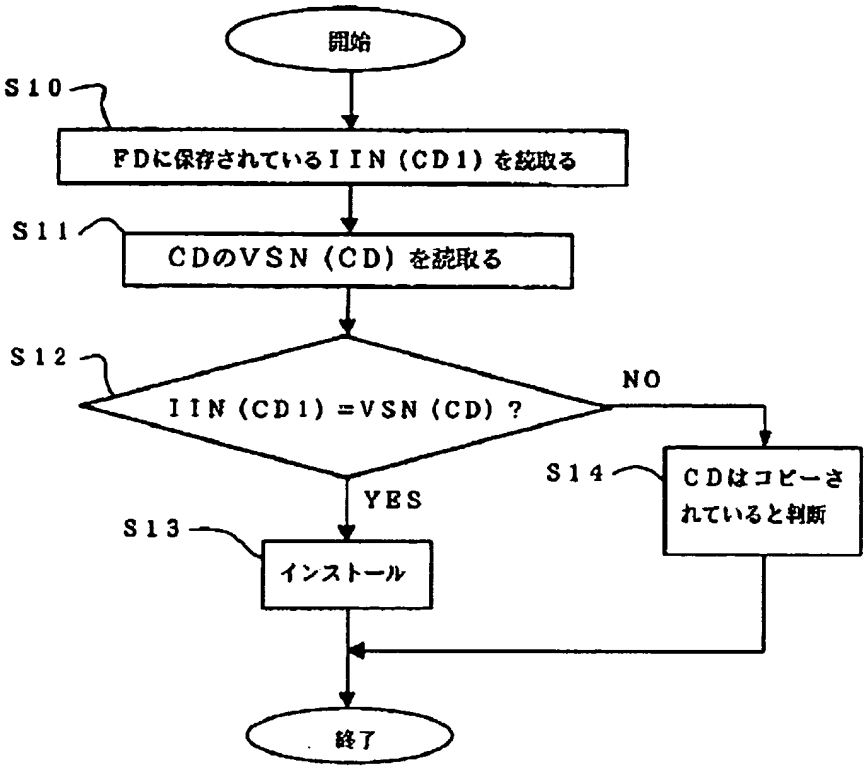



Figure 5 /18




[(A): Begin; (B): End; (S10): Decode IIN (CD1) saved in FD; (S11): Decode VSN (CD) of CD; (S13): Install; (S14): Judge the pervasion of copied CD]

Figure 6 /19

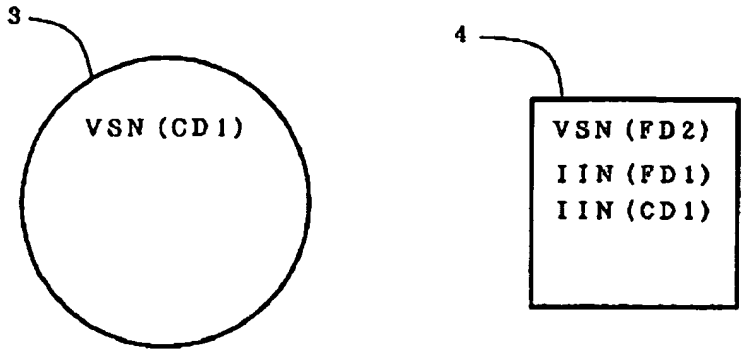
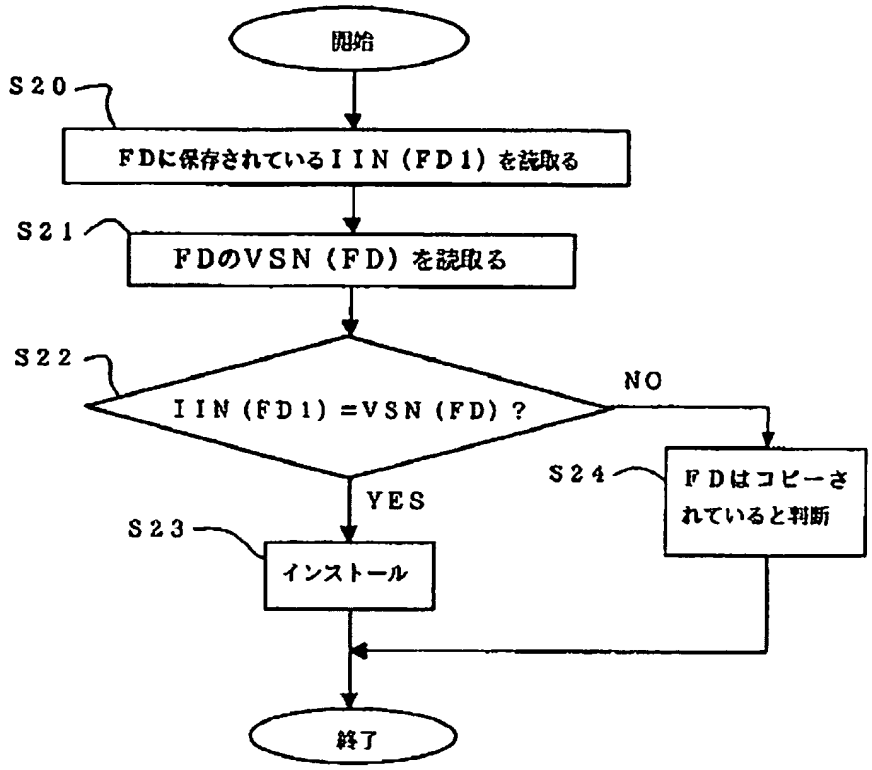


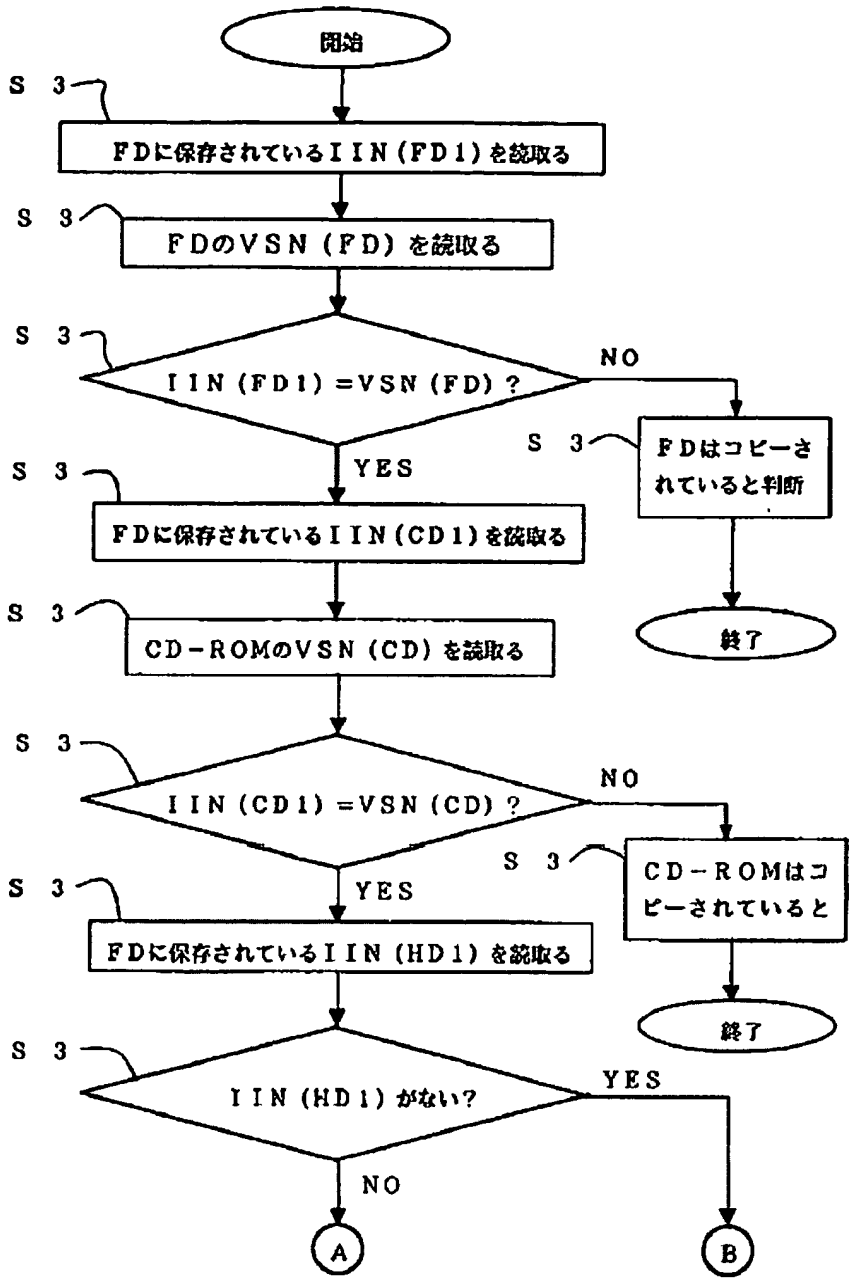

Figure 7 /20




[(A): Begin; (B): End; (S20): Decode IIN (FD1) saved in FD; (S21): Decode VSN (FD) of FD; (S23): Install; (S24): Judge the pervasion of copied FD]

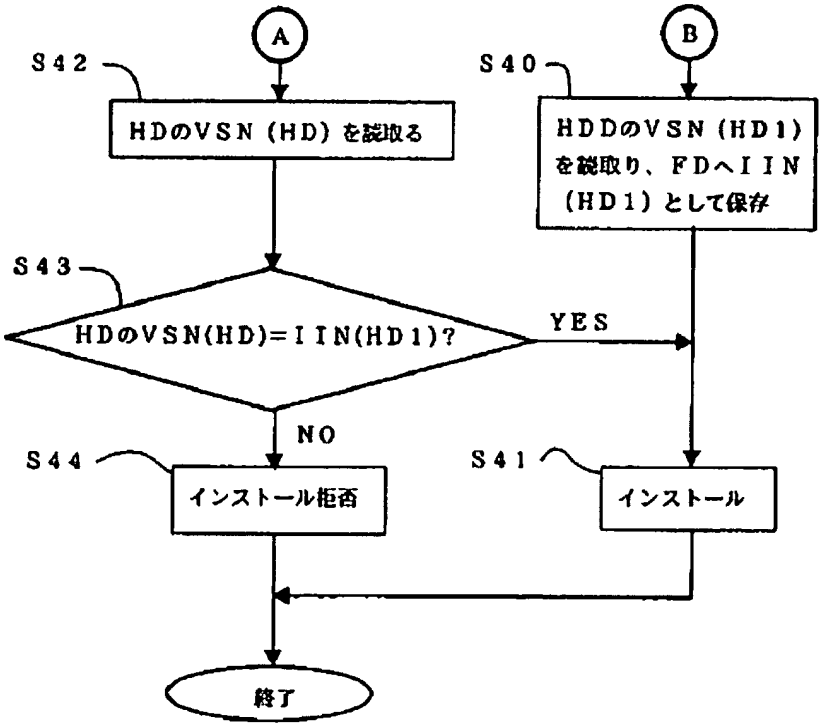
Figure 8 /21

第8図


開始
S 3
FDに保存されているＩＩＮ(FD1)を読取る
S 3
FDのＶＳＮ(FD)を読取る
S 3
ＩＩＮ(FD1)＝VSN(FD)？
NO
S 3
FDはコピーされていると判断
終了
YES
S 3
FDに保存されているＩＩＮ(CD1)を読取る
S 3
CD-ROMのVSN(CD)を読取る
S 3
ＩＩＮ(CD1)＝VSN(CD)？
NO
S 3
CD-ROMはコピーされていると
終了
YES
S 3
FDに保存されているＩＩＮ(HD1)を読取る
S 3
ＩＩＮ(HD1)がない？
YES
NO
A
B

[(A): Begin; (B): End; (S3[0]): Decode IIN (FD1) saved in FD; (S3[1]): Decode VSN of FD; (S3[3]): Judge the pervasion of copied FD; (S3[4]): Decode IIN (CD1) saved in FD; (S3[5]): Decode VSN (CD) of CD-ROM; (S3[7]]: Decode IIN (HD1) saved in FD; (S3[8]): [Judge] the pervasion of copied CD-ROM; (S3[9]): IIN (HD1) absent?]

Figure 9 /22




[(A): End; (S40): Decode VSN (HD1) of HDD & save same into FD as IIN (HD1); (S41): Install; (S42): Decode VSN (HD) of HD; (S44): Reject installation]